United Nations A/71/368

General Assembly

Distr.: General
30 August 2016

Original: English

Seventy-first session
Item 69 (b) of the provisional agenda*
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Right to privacy**

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on the right to privacy, Mr. Joseph A. Cannataci, in accordance with General Assembly resolution 68/167 and Human Rights Council resolution 28/16.

* A/71/150.
** The present report was submitted after the deadline to reflect the most recent developments.

16-14999 (E) 270916

Please recycle

Report of the Special Rapporteur on the right to privacy

Summary

The present report is the first submitted by the Special Rapporteur on the right to privacy to the General Assembly. It was written just over one year after the Special Rapporteur assumed the post on 1 August 2015 and precisely five months after the Special Rapporteur presented his first report to the Human Rights Council on 9 March 2016. Up to then, the Special Rapporteur had focused on identifying a number of themes which his many consultations with multiple stakeholders had revealed as being critical areas of work for the protection of privacy in the digital age.

In the intervening five months, the Special Rapporteur identified his first set of five priorities, as outlined in the present report, and on which he has commenced work in parallel. Those priorities are designated as Thematic Action Streams (TAS) on Big Data and Open Data; Security and Surveillance; Health Data; Personal data processed by corporations; and "A better understanding of Privacy". The methodology chosen by the Special Rapporteur is one which contemplates the setting up of a TASk force — some would call this a Working Party (WP) — composed of highly experienced and unpaid volunteers. One WP is being created for each of the five TAS, each of which is then expected to work on assisting the Special Rapporteur in researching and drafting a thematic study which would later form the subject of a report to the Human Rights Council or the General Assembly, to be presented during the period 2017-2018.

The Special Rapporteur is keen to maximize geographical distribution, cultural and ethnic diversity, stakeholder representation and gender balance in each of these TASk Forces or Working Parties. Thus, for example, the TASk Force on Big Data and Open Data will be chaired by David Watts, Commissioner for Privacy and Data Protection of the state of Victoria in Australia, while the TASk Force on Health Data will be chaired by Steve Steffensen, Chief of the Learning Health System at Dell Medical School in Austin, Texas, United States of America. At the time of writing, the Special Rapporteur was still going through the process of recruiting chairs and members for some of the TASk Forces. The precise composition of each TASk Force will be announced at an appropriate time, probably by March 2017. It is expected that each TASk Force will convoke meetings and also organize public, semi-public and behind-closed-doors events as appropriate in order to gather evidence and identify options for strategies which would produce improved safeguards and remedies for privacy in a given sector of activity.

Thus, the first event organized by the TASk Force on Security and Surveillance was the creation of the International Intelligence Oversight Forum (IIOF2016), in which the participation of several dozen oversight agencies and parliamentary committees is expected in Bucharest in October 2016. This will enable a collective identification of challenges to privacy and freedom of expression in the gathering of intelligence as well as best practices which could provide better safeguards and remedies therein. Meanwhile, the TASk Force on "A better understanding of Privacy" has already organized its first event in New York on 19 and 20 July 2016. It is intended that, of the five priorities, this TASk Force will report last, and certainly no earlier than 2018, since several other consultation events are expected to be needed in various regions, including Africa, Asia, Australia, Europe and South

America. The TASk Force has already started gathering evidence on concepts such as the relationship between privacy and an overarching fundamental right to the free development of personality. It is expected that its activities would constitute an ongoing process which would inform and learn from the findings of all the other TASk Forces set up by the Special Rapporteur.

While the five TASk Forces provide thematic focus, the Special Rapporteur has also continued monitoring developments within several dozen countries and has begun a programme of informal country visits that ensure the maximum possible interaction with the largest possible number of stakeholders during each visit. In the five months from March to August 2016, the Special Rapporteur participated in multiple activities, sometimes for a period of up to one week long, in 11 countries as diverse and as geographically far apart as Australia, Austria, Denmark, France, Germany, Italy, Latvia, the Netherlands, New Zealand, Switzerland and the United States. The next several months are expected to take the Special Rapporteur on both formal and informal country and area visits to France, Indonesia, Israel, Morocco, Northern Ireland (United Kingdom of Great Britain and Northern Ireland), sub-Saharan Africa, South America, Spain and the United States. This intense programme of work is carried out with the direct assistance of governments, privacy and data protection commissioners, human rights institutes, non-governmental organizations and universities.

Contents

		Page
I.	Introduction	5
	A. Starting off	5
	B. Initial feedback and follow-up initiatives	5
II.	Main activities carried out by the Special Rapporteur	5
	A. Resourcing the Special Rapporteur mandate	5
	B. Planning and setting up multiple activities in relationship to the mandate	7
	C. Engagement in multiple events	11
III.	Important developments and substantive issues, March-July 2016	13
	A. The right to silence *nemo tenetur se ipsum accusare*: should a smartphone be a compellable witness or is the potential privacy infringement too great?	13
	B. Data retention, mass surveillance and even more encryption	17
	C. More recognition of the relationship between privacy and personality	22
IV.	Conclusions	22

I. Introduction

A. Starting off

1. The present report is to be submitted to the United Nations for translation ahead of the October 2016 meeting of the General Assembly, on or around 9 August 2016, i.e., around 18 months since the Human Rights Council first established a mandate on the right to privacy in its resolution 28/16 and a year after the incumbent took up the appointment. At this point in time the Special Rapporteur confirms that the initiatives taken so far have received a lot of feedback, mostly of a positive nature. The present report will outline where the efforts of the Special Rapporteur have led so far and the main focus of activities in the near future.

B. Initial feedback and follow-up initiatives

2. A 10-point action plan was already presented in the first report to the Human Rights Council in March 2016 (see A/HRC/31/64, para. 46). The feedback received on the 10-point action plan was very positive. Hence, the Special Rapporteur will keep working on these issues and aim at presenting tangible results produced in cooperation with all stakeholders during the course of the mandate.

3. The experience gathered through the first 12 months of working on the mandate as well as in monitoring recent developments in the area have made it clear that some issues demand even more swift and decisive responses than others, and the first set of five priorities has thus been identified. The Special Rapporteur plans to take appropriate action and present outcomes from investigation into these priority areas in separate thematic reports.

II. Main activities carried out by the Special Rapporteur

A. Resourcing the Special Rapporteur mandate

4. Battles cannot be won if you have no troops to fight them with. Since the mandate is new, the Special Rapporteur walked into an administrative situation where no team existed, and has had to devote considerable time to seeking resources for his mandate outside the United Nations. Even had the quantity and quality of the resources provided by the United Nations been perfect — and they were not — there is no way that the job of the Special Rapporteur can be done properly without a considerable amount of resources over and above those provided by the United Nations. Monitoring the privacy legislation and the surveillance activities in over 190 States is a job which requires several dozen staff. Meeting civil society and understanding its concerns, as well as interacting continuously with corporations, law enforcement, intelligence agencies and policymakers, also requires a considerable investment in time and staff effort. Organizing consultation events in the five Thematic Action Streams outlined below also requires significant staff effort. Almost none of this staff effort currently comes from United Nations sources, especially since the type of staff required must possess domain expertise and be privacy specialists. Suffice it to say, at present some 90 per cent of the funding for staff assisting the work of the mandate and approximately 80 per cent of the travel-

related expenses incurred for the mandate had to be sourced from outside the United Nations. Furthermore, significant administrative hurdles within the system make it challenging to focus on the substantive part of the mandate.

5. When it comes to resources, to say that the support extended to the Special Rapporteur mandate by the Office of the United Nations High Commissioner for Human Rights (OHCHR) is far from satisfactory is a huge understatement. In line with the Latin maxim *contra factum non argumentum est*, let the facts speak for themselves:

(a) What the Special Rapporteur needs — and wants — is not general service bureaucrats but staff with domain expertise in privacy: the type of expertise which is only acquired through formal training, qualifications and direct experience. The Special Rapporteur made this point to the OHCHR Special Procedures senior management and indeed a call for applications for a post at the professional level (P-3) for a Human Rights Officer that indicated a preference for applicants with qualifications and experience in privacy was published in February 2016. The Special Rapporteur is advised that 349 applications were received in response to that call for applications but that at no time were the contents of these applications ever taken into account. The Special Rapporteur has not had sight of any of these applications but has been advised by some non-governmental organizations that they know of applicants with Ph.Ds. in privacy and several years of experience in privacy-related work;

(b) The senior managers at OHCHR with responsibility for the Special Rapporteur mandate proceeded to completely ignore the applications received in the public call for applications, and on 4 August 2016 informed the Special Rapporteur that a permanent Human Rights Officer had been appointed for the Special Rapporteur mandate holder from "an internal roster of candidates". This Human Rights Officer has no formal training or qualifications in privacy, no deep-seated experience/knowledge of privacy and only tangential experience in privacy matters. On 8 August the Special Rapporteur wrote formally to the Chair of the Human Rights Council requesting his intervention, distancing himself completely from this recruitment process and expressing his deep reservations about the equity of the process and its outcomes;

(c) Up to the time of writing, within the space of 12 months, the Special Rapporteur has been allocated a total of one Human Rights Officer at any one time, the current one being the third in a succession of temporary staff. There has been one occasion when, thanks to contractual complications, the Human Rights Officer was not available for an entire calendar month. None of the Human Rights Officers had formal training or qualifications in privacy or experience in dealing with privacy, though the latest Human Rights Officer allocated to the mandate (in July 2016), and who may turn out to be more permanent, has had some limited experience in dealing with privacy from the perspective of the mandate of freedom of expression. However personally pleasant or knowledgeable in other areas of human rights the allocated Human Rights Officers may have been, continuity and efficiency are very difficult to achieve and maintain in such circumstances;

(d) On 4 August 2016, the Special Rapporteur was advised that, in addition to the permanent Human Rights Officer mentioned in subparagraph (b) above, who would be made available full-time to the Special Rapporteur as at 1 September 2016, a half-time post at the P-3 level and a half-time post at the General Service

level (administrative assistant) would possibly be recruited during or after September. Given the level of efficiency demonstrated to date, we're not holding our breath;

(e) The level of inefficiency is such that partial reimbursements of costs for United Nations travel carried out in the fourth quarter of 2015 are still outstanding — and this to an unpaid officer like the Special Rapporteur.

6. The paucity of the support offered by OHCHR has been outlined in some detail (but in no way comprehensively) in the preceding paragraph in order to ensure that neither the General Assembly nor the Human Rights Council are left with any illusions that the Special Rapporteur is getting his work done thanks to some incredibly efficient or generous support from within OHCHR. I do not wish to return to this subject in future reports. If the Assembly or the Council does not hear from the Special Rapporteur again about the issue, they should assume that the situation has not improved in any way that would merit specific comment. On the other hand, this is not a blame-apportionment exercise: I will leave it to an incoming and hopefully reform-minded Secretary-General to decide whether the situation described in the preceding paragraphs is produced by a hopelessly inefficient system in dire need of overhaul and/or by a coterie of self-serving international civil servants who are far more keen to continue their cosy arrangements rather than give a Special Rapporteur the quality and quantity of the support required to properly carry out the mandate. If you represent a State or an organization which truly believes in the mandate and in its importance and wish to contribute, then kindly contact the Special Rapporteur directly in order to explore options for how further support could be provided.

B. Planning and launching multiple activities in relationship to the mandate

7. Despite the administrative and resource problems outlined above, the Special Rapporteur and his teams, supported by many actors from civil society and other stakeholders committed to the cause, were able to set in motion multiple activities. These may be broadly categorized as the ongoing monitoring of activities in individual States and Thematic Action Streams as further outlined below.

8. The development of new surveillance activities, laws enabling surveillance and privacy laws in several dozen United Nations Member States remains part of the essential ongoing monitoring activity carried out on a daily basis by the Special Rapporteur. This requires examining each new technology deployed and each new law proposed and investigating a number of complaints brought to the mandate holder's attention by the individuals concerned or by civil society. This monitoring activity is an essential part of the evidence-gathering process that informs the Special Rapporteur's choice regarding which countries to formally and informally visit.

9. In addition to country-specific activities, which are very time-consuming in themselves, much attention and effort have been directed to thematic priorities. Certain areas of the 10-point action plan submitted to the Human Rights Council in the report presented in March 2016 require immediate attention and concurrent action. These areas have been carefully identified and will now be dealt with in the

form of Thematic Action Streams (TAS).[1] In this first phase of activity, five TAS have been created, one for each of the following priorities: Big Data and Open Data; Security and Surveillance; Health Data; Personal data processed by corporations; and "A better understanding of Privacy". It is intended that each of these action streams will develop its own momentum while also interacting with other TAS and enable the Special Rapporteur to prepare a thematic report at the point where the investigation and debate within a specific TAS is mature.

A better understanding of privacy
Security and surveillance
Big Data and Open Data
Health Data
Personal data held by corporations

10. The methodology chosen by the Special Rapporteur is one which contemplates the setting up of a TASk force — some would call this a Working Party (WP) — composed of highly experienced and unpaid volunteers. There would be one WP for each of the five TAS, which would be expected to work on assisting the Special Rapporteur in researching and drafting a thematic study which would later form the subject of a report to the Human Rights Council or the General Assembly, to be presented during the period 2017-2018.

11. The prioritization of Big Data and Open Data was confirmed by secondary research and especially during multiple stakeholder meetings and fact-finding activities held during visits to Australia, Austria, Denmark, France, Germany, Italy, Latvia, the Netherlands, New Zealand, Switzerland and the United States of America during the period from March to July 2016. A TASk Force on Big Data and Open Data was therefore created in May 2016 with David Watts, Commissioner for Privacy and Data Protection of the state of Victoria in Australia, accepting the Special Rapporteur's invitation to chair the WP. Work commenced in June on devising a rough outline of the WP work objectives and recruiting the first members. On 20 July 2016, Mr. Watts and the Special Rapporteur presented the first

[1] More information on the subject can be found in the blog post of Joseph Cannataci, "Parallel streams of action (TAS) for the mandate of the United Nations Special Rapporteur for privacy and the first set of priorities", 3 June 2016. Available from https://www.privacyandpersonality.org/2016/06/privacy-and-personality-blog-3-parallel-streams-of-action-tas-for-the-mandate-of-the-un-special-rapporteur-for-privacy-and-the-first-set-of-priorities/.

outlines of proposed work at an event co-organized by the Special Rapporteur in New York, and invited comments and volunteers to work within the WP. Offers have since been received from volunteer experts hailing from Brazil, Canada, France, Senegal and the United States. It is expected that the composition of the TASk Force and the first outline of objectives and terms of reference will be published before the end of October 2016. Support is also being sought by this TASk Force from independent organizations wishing to help stress-test technical solutions which claim to successfully de-identify personal data in a such a way that re-identification will not be possible in the context of big data analytics capable of triangulation with Open Data sources.

12. There was never any doubt that Security and Surveillance would be high on the list of the Special Rapporteur's priorities. The complexity of the area, bringing together as it does interests from both law enforcement agencies and security and intelligence services, intersecting with the activities of a number of large corporations, has meant that it has been necessary to start by breaking the subjects to be tackled into smaller subsets, with the main emphasis throughout being on identifying and reinforcing privacy safeguards and remedies. The first major initiative taken by the Special Rapporteur in this sector was to create the International Intelligence Oversight Forum (IIOF2016), in which the participation of several dozen oversight agencies, parliamentary committees and intelligence services is expected to be held in Bucharest in October 2016. This should enable the collective identification of challenges to privacy and freedom of expression in the gathering of intelligence as well as best practices which could assist the Special Rapporteur and all the stakeholders in identifying better safeguards and remedies. Much preparatory work on organizing IIOF2016 was undertaken by the Special Rapporteur from March to July 2016, and the response from leading United Nations Member States has been very encouraging, with a number of States already having confirmed their participation in this meeting which, if successful, could be maintained as a regular event with ongoing input into the Special Rapporteur's reports, recommendations and other initiatives. The Special Rapporteur takes this opportunity to publicly thank those many United Nations Member States which have engaged with this exercise, especially the four Intelligence Oversight Committees of the Romanian Senate and Parliament which have accepted his invitation to co-host the event. Thanks are also due to the European Union Agency for Fundamental Rights, which is supporting this event in various ways. Further work on surveillance is also being carried out in the context of the TASk Force on Personal data processed by corporations (see below). Other initiatives and work in the sector may be made public at a later date.

13. The Special Rapporteur's constant interaction with stakeholders and in-depth research has confirmed that the creation, processing, sale and resale of vast amounts of sensitive health data continues to grow worldwide. Not only is this institutionalized as part of the business model in a small number of trend-setting countries, but it is also being exacerbated by the upward-spiralling trend by consumers to use wearables, smartphone apps and other portable technologies which constantly gather and transmit many forms of potentially sensitive health and lifestyle data. Furthermore, experiments in some countries with the use of existing medical health records to provide better diagnostic capabilities thanks to artificial intelligence techniques may also prove to be a growing source of concern. On the other hand, it is clear that there may be a number of benefits, including advances in

medical research, in the use of health data. Some independent market research also suggests that patients are increasingly concerned that their personal data could be misused. In order to take his efforts in the health data sector forward in a structured manner, and following a period of consultation with leading non-governmental organizations in this area, the Special Rapporteur is pleased to announce that Dr. Steve Steffenson of Dell Hospital at the University of Texas in the United States has accepted to chair the Working Party dubbed MedITAS. The other members of the WP are currently being recruited and the preliminary terms of reference which have been drawn up are expected to be developed further and adopted once the TASk Force becomes operational by early in the fourth quarter of 2016.

14. The Special Rapporteur is building on his engagement with leading corporations achieved through previous and ongoing projects and especially with the European Union-supported Managing Alternatives for Privacy, Property and Internet Governance (MAPPING) project in order to continue to examine the privacy impact of the growing use of personal data by the corporate sector. The Special Rapporteur continues to benefit from ongoing work with corporations on at least three tracks within the MAPPING project dealing with the potential of international law, business models and privacy, which are expected to provide further input into the mandate holder's work in this sector as well as shape (within the MAPPING project) a policy brief and a road map for the European Union to consider. Some of this work is also relevant to government surveillance activities and is expected to lead to a joint consultation on the matter with civil society in an event to be organized on 15 and 16 February 2017, co-organized by the Special Rapporteur mandate holder and the MAPPING project. Thanks are due to a number of leading companies, including Microsoft, Google, Facebook, Apple and Yahoo!, as well as the Global Network Initiative, which have continued to engage with the Special Rapporteur's mandate as well as the MAPPING project in a very welcome manner. All other stakeholders are welcome to join this process at the appropriate time and the Special Rapporteur invites expressions of interest in this matter, as in all other TASk initiatives.

15. One of the longer-term initiatives taken by the Special Rapporteur is the TASk Force focused on "A better understanding of Privacy". The intention is that, of the current set of five priorities, this TASk Force will report last, and certainly no earlier than 2018, since several other consultation events are expected to be needed in various regions, including Africa, Asia, Australia, Europe and South America. This TASk Force has already started gathering evidence on concepts such as the relationship between privacy and an overarching fundamental right to the free development of personality. It is expected that its activities would constitute an ongoing process which would inform as well as learn from the findings of all the other TASk Forces set up by the Special Rapporteur. It is also one of the TASk Forces which devotes considerable attention to the relationship between privacy and other fundamental rights such as freedom of expression and freedom of (access to) information. Preliminary discussions with Human Rights Watch as early as September 2015 developed a momentum which led to the organization of the first event by this TASk Force, entitled "Privacy, personality and flows of information" in New York on 19 and 20 July 2016. This two-day event filled a 90-seat conference room to capacity and was held thanks to the generosity and combined efforts of Human Rights Watch; the Brennan Center for Justice at the New York University School of Law; Global Freedom of Expression at Columbia University; the

MAPPING project; the Department of Information Policy and Governance of the University of Malta; and STeP, the Security, Technology and e-Privacy Research Group at the University of Groningen in the Netherlands. Thanks are also due to the Government of Germany for providing the mandate holder with some of the funds which supported worldwide participation in this event.

16. While clearly the local (United States) perspective was best represented, participants from Australia, Brazil, Canada, Colombia, India, the Republic of Korea, the Middle East and North African region, Europe[2] and the United Nations Educational, Scientific and Cultural Organization were also present to share their views and insights. The main aim of the meeting during the first day was to work on a more comprehensive and better understanding of what privacy means as a universal human right in the digital age and whether the right has to be understood more strongly in the context of enabling personal development. The second day was focused on facilitating the understanding and development of advocacy strategies in order to enable the more effective and strong promotion of the right to privacy globally. This event successfully served as a pilot for a new series of events which will deal with the same subject and will be organized on all continents to consolidate as many views as possible on the subject in order to aim at establishing and deepening a more comprehensive understanding of privacy and its interpretation in the digital age for the benefit of the global community. Therefore, while the planning for the next event, to be held in Asia, has already started, the Special Rapporteur would like to hereby invite any parties interested in supporting, hosting and participating in such events in the near future to contact him directly.

17. Largely (but not exclusively) as part of the work undertaken to support the mandate, the Special Rapporteur and his team have also set up a blog on the topic of privacy and personality. It can be accessed at www.privacyandpersonality.org.

C. Engagement in multiple events

18. Apart from the activities outlined above, and also in pursuit of the privacy awareness objective outlined in the 10-point action plan, the Special Rapporteur has participated in a number of activities since 3 March 2016, including:

(a) Keynote speech, Institute for International Law of Peace and Armed Conflict, held in Bochum, Germany, on 15 March;

(b) Meeting with the President of the Commission Nationale de l'Informatique et des Libertés and the Chair of the Article 29 Working Party of the European Union, held in Paris on 18 March;

(c) Panel participation, International Association of Privacy Professionals Global Privacy Summit, held in Washington, D.C., on 5 April;

(d) Keynote speech, annual symposium of the Wisconsin International Law Journal, held in Wisconsin on 8 April;

[2] Specifically, the German understanding of "information self-determination" and privacy protection ("datenschutz") was considered and discussed as a potential blueprint to develop the understanding of privacy as an enabling right to develop personality. The Special Rapporteur is grateful for a contribution from Christian Hawellek from the Institut für Rechtsinformatik at the Leibniz Universität Hannover.

(e) Keynote pre-conference, Association Data Protection Officer (ASSO DPO) annual congress (workshop focused on the General Data Protection Regulation and the role of the Data Protection Officer of the European Union), held in Milan, Italy, on 18 April;

(f) Global Digital Futures Forum, Columbia University, held in New York on 25 April;

(g) Multiple keynote speeches and stakeholder meetings, Privacy Week, New Zealand, held in Wellington and Auckland from 9 to 13 May;

(h) Multiple keynote speeches and stakeholder meetings, Privacy Awareness Week, Australia, held in Sydney and Canberra from 14 to 18 May;

(i) Security Research and Innovation event 2016, held at The Hague on 1 and 2 June;

(j) Panel: "Privacy in the next administration", "Data Protection 2016" conference, Electronic Privacy Information Center (EPIC), held in Washington, D.C., on 6 June;

(k) Keynote speech, Sixth International Summit on the Future of Health Privacy, held in Washington, D.C., on 7 June;

(l) MAPPING and Special Rapporteur stakeholder event, organized by Alvaro Bedoya at the Georgetown Law Center for Privacy, held in Washington, D.C., on 8 June;

(m) Meetings with Google, Facebook and the Department of State of the United States, held in Washington, D.C., on 9 and 10 June;

(n) Open lecture and keynote speech, DataEthics.EU and Danish Institute of Human Rights, held in Copenhagen on 13 June;

(o) Round table, Association of Progressive Communications, held in Geneva on 14 June;

(p) Intervention, workshop organized by the International Committee of the Red Cross, held in Geneva on 14 June;

(q) Online discussion with members of the Internet Society, held in Geneva on 14 June;

(r) "Convention 108: from a European reality to a global treaty", Council of Europe, held in Strasbourg, France, on 17 June;

(s) Fundamental rights forum, European Union Agency for Fundamental Rights, held in Vienna on 20 and 21 June;

(t) Alpbach Talks: "Time to share: places for everyone", in cooperation with *Wiener Zeitung*, held in Vienna on 22 June;

(u) "The role and responsibility of business in respecting privacy in a context of increased security in Europe", Working group 25, held in Vienna on 23 June;

(v) Second European Media and Information Literacy Forum, held in Riga from 27 to 29 June;

(w) "Privacy, personality and flows of information", conference of the Special Rapporteur on the right to privacy, held in New York on 19 and 20 July.

III. Important developments and substantive issues, March-July 2016

A. The right to silence *nemo tenetur se ipsum accusare*: should a smartphone be a compellable witness or is the potential privacy infringement too great?

19. The year 2016 has seen the return of a debate on the value of encryption of personal data stored on or generated by mobile devices. Arguably most prominently, the events relating to a smartphone used by a person who committed a terrible attack in San Bernardino, United States, and the following attempts of United States authorities to gain access to personal data stored on the device manufactured by Apple Inc. have caught public attention. On 2 December 2015, a husband and wife opened fire on a local government office in southern California. As a result, 14 people were killed and more than 20 people seriously injured.[3] The United States Federal Bureau of Investigation (FBI) was interested in information that had been stored on the device and synched with Apple's cloud computing service (iCloud). While it was possible to retrieve the data stored externally until 19 October 2015 (when the backups stopped), the data that was stored locally on the smartphone was not easily accessible to the FBI or to Apple. The FBI tried to use the legal framework to create an obligation by Apple to change the software on the smartphone in order to make it less resilient in the case of a hacking attack. When Apple refused to accede to the demand, the FBI took the case to court and applied pressure on the company. Ultimately, on 28 March 2016, the FBI dropped its court fight against Apple because it became possible to gain access to the information stored on the smartphone by other means.[4] "From the beginning, we objected to the FBI's demand that Apple build a backdoor into the iPhone because we believed it was wrong and would set a dangerous precedent. As a result of the government's dismissal, neither of these occurred," Apple said in a statement following the dropping of the case.[5] The Special Rapporteur has, in paragraph 30 of his report of 9 March 2016, outlined his position that permitting or mandating back doors to encryption is a bad idea for many reasons, best summarized in a position paper of the Government of the Netherlands of 4 January 2016. The Apple case has done

[3] Camila Domonoske, "San Bernardino shootings: what we know, one day after", *National Public Radio*, 3 December 2015. Available from www.npr.org/sections/thetwo-way/2015/12/03/458277103/san-bernardino-shootings-what-we-know-one-day-after.

[4] See the following articles from *The Guardian*: Danny Yadron, Spencer Ackerman and Sam Thielman, "Inside the FBI's encryption battle with Apple", 18 February 2016. Available from https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple; Danny Yadron, "San Bernardino iPhone: United States ends Apple case after accessing data without assistance", 29 March 2016. Available from https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone; Danny Yadron, "FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone", 28 April 2016. Available from https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino.

[5] Hilary Brueck, "This is Apple's response to the FBI hacking into that iPhone", 29 March 2016. Available from http://fortune.com/2016/03/29/apple-response-fbi.

nothing to change his mind about that aspect of the matter. Smartphones and other mobile devices do, however, raise other fundamental rights issues which may have an impact on privacy and which may possibly need to be decided before the next phase of the "conversation" about encryption can take place or move forward effectively. One such right is the right to silence.

20. Now that the Apple versus FBI case is no longer sub judice and, hopefully, people on all sides can think a bit more clearly and less passionately, it is respectfully submitted that since hundreds of millions of Apple smartphones have been sold globally this is a global issue and not one which is of interest solely in the United States. Likewise, the same laws which were used to try and compel Apple to help law enforcement agencies obtain access to the data in that case may be used with other manufacturers who have sold many more hundreds of millions of smartphones around the world than Apple has, especially since more and more manufacturers are building cryptographic safeguards into their products. It would appear that economies of scale mean that we are moving towards a situation where first one third and eventually half of the world's population will own and use a smartphone. Thus, as will be seen below, we are faced with a simple fact: the smartphone is a ubiquitous technology which has huge ramifications for privacy.

21. The Special Rapporteur will here outline some preliminary observations in an attempt to move the debate about smartphones beyond privacy, with the intent of eventually moving the debate back to core privacy concerns better informed by the confirmation or abnegation of societal values regarding "the bigger picture". It is the Special Rapporteur's position that other appropriate standards of behaviour need to be examined within society before a more definitive view can be taken about some of the privacy dimensions of smartphone use.

22. Like many other fundamental human rights, privacy is a dynamic right, not a static right. An expectation of and a preference for privacy has existed for thousands of years, but this does not mean that the degree of protection of the right or the understanding of the boundaries of the right have remained unchanged as the direction has moved to greater protection. Privacy has developed over time, and much evidence has been identified prior to the creation of the Special Rapporteur mandate and the appointment of the incumbent which shows how the understanding of privacy and the exercise of the right has varied across the dimensions of "Time, Place and Space".[6] Contrary to what some may think, recognizing this reality does nothing to undermine the existence of the right nor its universality. Instead, it makes one reflect about the complex set of values that underpin the right and the way that our understanding of the right needs to change as circumstances change in order for the underlying values to continue to be protected and indeed, as much as possible, have their protection increased. The advent and applications of new technologies such as the smartphone is one typical example of how we need to update our understanding of privacy. As United States Supreme Court Justice Samuel Alito put it, in the landmark United States case of *Riley v. California* in 2014:

> We should not mechanically apply the rule used in the predigital era to the search of a cell phone. Many cell phones now in use are capable of storing and

[6] For a much more detailed insight into the Special Rapporteur's assessment of the existence and time, place and space dimensions of privacy across the millennia, see Joseph A. Cannataci, ed., *The Individual and Privacy* (Farnham, United Kingdom, Ashgate Publishing, 2015).

> accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form.[7]

In this, Alito is concurring with the majority opinion as expressed by Chief Justice John Roberts that:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life". The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.[7]

Needless to say, it is not just Americans who wittingly or unwittingly surrender "the privacies of life" to their cell phones. Indeed, every single person on earth who carries a smartphone has entrusted to their most used portable device the privacies of their life irrespective of their creed, colour, ethnic origin, gender, nationality or geographical location. Which is why many of the observations made in *Riley v. California* are also of global importance. The Special Rapporteur will here quote extensively from this United States case since it outlines some of the arguments which should be considered next in the overall context of the dispute between Apple and the FBI wherever such issues are raised across the globe.

23. As outlined in *Riley v. California*: "Modern cell phones ... are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[7] The Supreme Court Justices noted correctly that:

> Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers. One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.[7]

More than once the United States Supreme Court Justices note that:

> There is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smartphone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower.[7]

The ability of the smartphone to provide a very detailed and accurate profile of its user is likewise identified by the Justices:

---

[7] Supreme Court of the United States of America, *Riley v. California*, Decision of 25 June 2014, No. 13-132. Available from https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns — perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been.[7]

24. Most important, perhaps, is the realization by the Justices of the United States Supreme Court that the contents of a cell phone are so large in quantity and intimately private in character that they go far beyond the level of privacy that would be intruded upon in a traditional search of one's home as protected by the Fourth Amendment to the United States Constitution:

> A cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form — unless the phone is.[7]

In this way, the Justices of the United States Supreme Court showed how the new technology embodied by smartphones has been a game shifter and that at this moment in "Time" (2014), the "Place" (the United States — and the phone located in the United States) where the personal data was to be found had changed significantly to one where portability, quantity and quality of the personal information are capable of completely altering and intensifying the privacy dimension of the personal "Space".

25. The United States Supreme Court Justices in *Riley v. California* were primarily concerned with outlawing warrantless searches of smartphones in terms of privacy considerations inherent in the Fourth Amendment to the United States Constitution. It is relevant to point out, however, that the situation regarding cell phone security and encryption may be significantly more complex than one solely revolving around arguments of privacy and security. It may only be a matter of time before the United States Supreme Court Justices are faced with the same dilemma that would face the scores of countries around the world which have recognized the right to silence or the right to avoid self-incrimination as one of the standards of decency that a democratic society subscribes to. This is because the very characteristics of a mobile phone which make it such a special repository of personal data, as outlined in *Riley v. California*, also make it the most obvious tool which could totally and effectively undermine the right to silence, which has been gradually recognized in various jurisdictions since the sixteenth century and which in the United States is recognized as the Fifth Amendment. Put simply, in many jurisdictions around the world — but not all — an accused person has the right to avoid self-incrimination by remaining silent during criminal proceedings against him or her. There are very few exceptions to or qualifications of this right in places as far apart as Australia, Bangladesh, Germany, India, New Zealand, the United States ... the list goes on. Yet a judicial warrant to access data held on a phone could effectively breach that right. The accused — hitherto not a compellable witness — may have the right to remain silent, but his or her phone could speak volumes about the most private of his or her thoughts, interests and actions. The accused's spouse or close family may equally be afforded the same status of not being a compellable witness in many

jurisdictions. Yet most people would claim that their smartphone knows much more about them than their spouses, so is the smartphone to remain a compellable witness even with a judicial warrant required to access it? So where should logic — and logical consistency — lead us to?

26. At the present moment in time the Special Rapporteur on the right to privacy is identifying this issue of the smartphone and similar devices (including wearables and implants) as one for future discussion, possibly by or in collaboration with other Special Rapporteurs. No particular opinion or recommendation is being made by the Special Rapporteur at this preliminary juncture. At this stage, it is simply a question of identifying a subject for further investigation as a matter which impinges strongly on privacy, but is not only of interest exclusively to the right to privacy but also to other fundamental rights such as those of due process in criminal proceedings. Some might argue that the logical conclusion of *Riley v. California*, when applied to the right to silence as distinct from the right to privacy, would mean that in most cases the smartphone of the accused in criminal proceedings should not be a compellable witness — a position which would then also have a significant impact on the right to privacy, certainly insofar as it would be a recognition of how intimate and private the data held on the smartphone might be.

27. The United Kingdom of Great Britain and Northern Ireland, where, ironically, the origins of the right to silence may be traced for well over four hundred years, has actually taken the position that national security or the suppression of crime trumps privacy or the right to silence when it comes to electronic devices. In terms of sections 49 and 53 of the Regulation of Investigatory Powers Act 2000, it is an offence to fail to disclose the key to encrypted data when requested (with a penalty of two years in prison, or five years with regard to child sex abuse cases). Therefore, not only is the smartphone a compellable witness in the United Kingdom, but if you don't provide the keys to the device you could also be looking at an additional jail sentence. The case of Apple versus the FBI was slightly different in that the accused were actually dead and there was no doubt as to their culpability, but rather that access to the phone was required to get the bigger picture in terms of facts and the preparation of the terrorist act, as well as associates and connections in what could be a national or international terrorist network. The interest that the case has raised, however, is justly deserved because it takes us to the heart of discussions about privacy, security and the right to silence. Perhaps the next step would be to organize a study at the intersection of the right to privacy and the right to silence. The Special Rapporteur will consult with the International Bar Association, European bar associations and various other stakeholders before forming a view as to whether the time is ripe for an in-depth investigation and whether recommendations for evidence-based policymaking in this field are required.

B. Data retention, mass surveillance and even more encryption

28. Despite the rulings of numerous national constitutional and regional human rights courts, the Special Rapporteur observes that there is an increased tendency for governments to promote more invasive laws for surveillance, which allow for the thinly disguised permanent mass surveillance of citizens.

29. Moves in this direction continue with the passage of the third reading of the Investigatory Powers Bill in the House of Commons of the United Kingdom. The

Bill is scheduled to continue to be considered at the Committee stage in the House of Lords in September 2016. The Special Rapporteur must assume that readers are also familiar with the criticism he made of the Bill in his report of 9 March 2016. The part of the Bill which deals with mass surveillance and bulk hacking continues to be under international scrutiny. The Court of Justice of the European Union is set to rule on the matter following an opinion expressed by the Advocate General of the Court, on 19 July 2016, that bulk processing is only legal in cases of serious crime, which is a far narrower use than that permissible under the Bill. The Bill remains a privacy minefield, a thorough analysis of which would require 10 times the 10,300 word limit that the present report must respect, but the battle is happily being valiantly fought by Ministers of Parliament, Liberty, the Law Society, the Open Rights Group and Privacy International. It can only be hoped that the Government of the United Kingdom presses the pause button, listens carefully to what both the European Court of Human Rights and the Court of Justice have to say about surveillance and lets sanity prevail. It would also do well to listen to some members of its own House of Lords. Lord Paddick, a former senior police officer, has lambasted the Bill's provisions dealing with Internet connection records, saying: "Internet connection records — the only virgin territory in the Bill — are going to intrude into innocent people's privacy." He later argues that the catch-all nature of Internet connection records is disproportionate given the warrantless access the Bill affords to police of this personal data on all Internet users in the United Kingdom.[8]

30. Never mind that the Investigatory Powers Bill should never have been proposed in its current form nor advanced to approval by the House of Commons in the first place. The discussion in the House of Lords to date has not been encouraging. Earl Howe, Minister of State for Defence and Deputy Leader of the House of Lords, on 13 July 2016, said:

> It may be entirely sensible for the government to work with [communication service providers] to determine whether it would be reasonably practicable to take steps to develop and maintain a technical capability to remove encryption that has been applied to communications or data.
>
> Law enforcement and the intelligence agencies must retain the ability to require telecommunications operators to remove encryption in limited circumstances.[9]

31. Statements such as these suggest one of four options: (a) the Minister is being badly briefed; (b) the Minister is being briefed by people who do not understand how encryption really works; (c) the Minister does not understand the brief; or (d) the Minister is deliberately misrepresenting the situation to the House of Lords. The Special Rapporteur does not wish to believe that this is a case of deliberate misrepresentation and therefore appeals to the Noble Lord and all his fellow members of the House of Lords to get on top of a few simple facts. Perhaps if the members of the House of Lords were to understand the arguments presented by the Government of the Netherlands on 4 January 2016, they would then understand why attempts to legislate weakened encryption into being are a bad idea and particularly

[8] House of Lords of the United Kingdom of Great Britain and Northern Ireland, Investigatory Powers Bill debate of 27 June 2016, vol. 773. Available from https://hansard.parliament.uk/lords/2016-06-27/debates/1606278000466/InvestigatoryPowersBill.

[9] Ibid., Investigatory Powers Bill debate of 13 July 2016, vol. 774. Available from https://hansard.parliament.uk/lords/2016-07-13/debates/16071337000437/InvestigatoryPowersBill.

daft in practice. They would understand that, far from being "entirely sensible", such proposals are entirely nonsensical. They would also understand why statements such as "Law enforcement and the intelligence agencies must retain the ability to require telecommunications operators to remove encryption in limited circumstances" are illusory and a far cry from reality. Law enforcement and intelligence agencies in most cases emphatically do not have the ability to require telecommunications operators to remove encryption — or else they may require them to do so until they are blue in the face — for the simple reason that in most cases the telecommunications operators do not have that ability in the first place. If the Parliament of the United Kingdom were to be misguided enough to approve such a particularly nonsensical piece of legislation, it would only require a very small effort for an individual to download any number of encryption algorithms/encrypted communications programmes produced outside either the United Kingdom or the United States, but freely available on the Internet, and then use such programmes to communicate with others intent on causing harm inside the United Kingdom. There is nothing a telecommunications operator can do in such circumstances and nothing more a signals intelligence agency can do than try to crack the code.

32. Some members of the House of Lords do understand the issue perfectly. Lord Strasburger put it quite succinctly:

> One feature of end-to-end encryption is that the provider cannot break it; encryption is private between the users at both ends. [Earl Howe] seems to be implying that providers can use only encryption which can be broken and therefore cannot be end to end, so the next version of the Apple iPhone would in theory become illegal. I think that there is quite a lot of work to be done on this.[9]

The Special Rapporteur thinks so too, and would suggest that much of the work that needs to be done lies in the direction of moving the Government of the United Kingdom away from the illusion that it can effectively outlaw end-to-end encryption or make it unavailable to persons inside the United Kingdom. This proposal is on the same level of illogical thinking as trying to ban knives altogether because they could occasionally be used for harm, or to ban cars because they are sometimes used as getaway vehicles. Moreover, the security risks introduced by deliberately weakened encryption are vastly disproportionate to the gains. Strasburger summarized:

> I want to emphasise — and anybody in the cryptography industry will spell this out — that you cannot have it both ways. Either encryption is secure, or it is not; it cannot be insecure for a small group of users and secure for everybody else.[9]

Lord Paddick pointed to an approach which would be more consistent with the case law of the European Court of Human Rights as last expressed in *Zakharov v. Russia*: "Instead of the power to force a company to remove encryption from a whole service or technology, alternative and more targeted powers should be used instead."[9] The Special Rapporteur can, at the present stage, only wonder when common sense — never mind a deserved respect for fundamental human rights like privacy — will finally prevail in the State's debate on the subject.

33. Germany has, for decades, provided an excellent example in pioneering privacy protection in some areas. In April 2016, the Constitutional Court of Germany kept true to this tradition when it ruled that parts of a law ("BKA-Gesetz") granting surveillance powers to federal police were unconstitutional because they did not have sufficient safeguards to ensure a balance between the rights of the individual to privacy and the interests of the State in investigating potential crime. Certain powers, such as the ability to conduct surveillance through recorded conversations or photographs, to carry out wiretaps or to remotely search computers, did not have adequate restrictions, including the possibility of judicial review, to guarantee that intrusions on the privacy of German citizens would be justified and proportionate, the court found.[10]

34. The democratic oversight of intelligence services in Germany remains a cause for concern. The Special Rapporteur shares the concerns of Nils Muižnieks, the Commissioner for Human Rights of the Council of Europe, and notes that his findings of October 2015 have not been contradicted. In particular, that:

> Current challenges relating to effective oversight of intelligence and security services in Germany include the lack of resources and expertise, the scope of the oversight of telecommunications, problems of coordination, as well as the absence of effective remedies for persons affected by surveillance of their telecommunications.

The Commissioner is particularly concerned by the lack of resources and technical expertise of the oversight bodies and their secretariat. In this respect, the ratio of the number of overseers to the number of those subject to oversight is especially telling: two bodies of 13 members, supported by a small secretariat, are responsible for the oversight of activities involving, for the largest agency (the BND), a staff of about 6,000.[11]

> It is the Special Rapporteur's intention to follow up such concerns in various forums, including IIOF2016 and, at the appropriate moment, directly with the Government of Germany.

35. On 28 June 2016, the Government of Germany signed off on a draft law on the Federal Intelligence Service (the Bundesnachrichtendienst, or BND) that amended several existing laws containing provisions on the surveillance of non-German citizens outside of Germany. On 8 July 2016, the draft law passed its first reading in Parliament. It is expected that two remaining readings of the draft law, including the final vote, could take place as early as the fourth quarter of 2016.

36. The first observation to be made here revolves around the issue of nationality, with the draft law continuing to make distinctions between German and non-German citizens. The way this reflects reality is not clear at all. Most of the terrorist attacks carried out in Europe during the past two years and more were carried out by European Union citizens, most often by citizens of the State where the attack was carried out. If the major risk lies there, (i.e., with the citizens of one's

[10] Wenzel Michalski, "Dispatches: rare victory for privacy in Germany's 'war against terror'", Human Rights Watch, 27 April 2016. Available from https://www.hrw.org/news/2016/04/27/dispatches-rare-victory-privacy-germanys-war-against-terror.

[11] Council of Europe, "Report by Nils Muižnieks, Commissioner for Human Rights of the Council of Europe: following his visit to Germany on 24 April and 4 to 8 May 2015", 1 October 2015. Available from https://www.ecoi.net/file_upload/1226_1447235185_commdh-2015-20-en.pdf.

own State) what is the true value of laws that discriminate between nationals and non-nationals? Especially since, in terms of article 17 of the International Covenant on Civil and Political Rights, everybody enjoys a right to privacy irrespective of nationality or citizenship, so one must ask how useful and appropriate, never mind legal, such types of provisions may be. This anomaly was also noted by Mr. Muižnieks, who reported that: "According to the authorities, the protection afforded by Article 10 of the Basic Law does not extend to activities outside Germany and is limited to German citizens or activities taking place in Germany." This interpretation is as unacceptable as any claim in the laws of other countries that fundamental human rights protection is only restricted to its own citizens or residents. Indeed, Mr. Muižnieks reported also that:

> This interpretation is however disputed since the Federal Constitutional Court ruled in 1999 that the protection afforded by the Basic Law is not limited to Germany's territory and fundamental rights have to be respected, at least when information that was obtained abroad is processed in Germany.[11]

The new draft German law loses out on a precious opportunity to clarify that the right to privacy and related safeguards applies to individuals irrespective of nationality, citizenship or location, or indeed whether the surveillance is carried out inside or outside Germany.

37. Furthermore, the draft German law raises a whole plethora of other concerns:

(a) Purpose specification: the conditions for the collection and processing of data are vague and too broad;

(b) Mass surveillance: mass and targeted surveillance of extraterritorial communications between non-German citizens would be effectively authorized in cases where the communication interception is carried out in Germany. While targeted surveillance in line with the criteria outlined in *Zakharov v. Russia* is of less concern, mass surveillance remains a cause for grave concern and prima facie runs counter to the standards established in European law;

(c) Independent oversight: the new law contains no adequate independent judicial oversight;

(d) The level of resourcing of oversight of the proposed mass surveillance under the draft law is hopelessly inadequate and of the wrong type. The new law envisages a three-member committee that is only required to meet four times a year and which may not have sufficient staff or resources to oversee mass surveillance operations that are, by their very definition, extensive in scope. This leaves the Special Rapporteur in exactly the same zone of concern as that expressed by Mr. Muižnieks. Moreover, given that the appointment and composition of the membership comes from the executive does nothing to strengthen the impression of independent oversight.

38. In the light of the above, the new draft German law prima facie suggests that the German authorities have not learned anything from the October 2015 report by Mr. Muižnieks. Instead of providing the Special Rapporteur with a model law which can be used as an example of good practice around the world, the Government of Germany has come up with something which is worse than disappointing. With all its many defects, the United Kingdom draft Investigatory Powers Bill at least attempted to partly rectify the weak oversight regime previously criticized by the

Special Rapporteur and others. While far from perfect, the new proposed oversight regime in the United Kingdom would appear to be an improvement over the previous situation. Not so in Germany which, unless it pulls back from the brink and radically changes course, promises to take over the position hitherto held by the United Kingdom as the country with the weakest oversight regime in the western world in proportion to the size of its intelligence services.

39. While the Special Rapporteur can understand the anxiety induced by the recent spate of attacks in Germany, he continues to look to that country for leadership in the field of privacy and data protection and extends an offer, as in the case of the United Kingdom, to work with the Special Rapporteur to produce a new law and an adequate oversight resource regime which would serve as an example of best practice globally.

C. More recognition of the relationship between privacy and personality

40. The National Institute for Transparency, Access to Information and Protection of Personal Data (INAI) of Mexico issued a very interesting judgment (Expediente PPD.0050/16) on 13 July 2016, where we read that: "It is pertinent to note that although the right to the protection of personal data, in accordance with its constitutional regulation, is an autonomous right to the protection of private life, there should be a broader interpretation of both concepts, while the latter means a sphere where anyone can freely develop their personality." Therefore, in general, the protection of private life includes other rights and specific guarantees for the storage of information, access to personal data, as well as the regulation on protection of private communications, names, physical and moral integrity.

IV. Conclusions

41. In the first full year of office, the Special Rapporteur has visited 14 countries during 20 trips undertaken for the mandate holder's business. These have included visits to countries as geographically far apart as Australia, Brazil, New Zealand and the United States, as well as 10 European States. Although technically speaking these were "informal" country visits, on many occasions they included the full array of engagements carried out during traditional official visits of the Special Rapporteur, including meetings with ministers, ministry officials, intelligence services, oversight agencies, data protection commissioners, law enforcement, civil society and leading corporations. In an overwhelming number of cases, the Special Rapporteur was received in a very positive manner. The next 12 months will also include at least two and possibly three official country visits, all tentatively scheduled, one each on three different continents (Africa, Asia and Latin America).

42. The Special Rapporteur has launched a system of structured consultations around the world. Civil society, individuals, governments, corporations and other stakeholders have registered their interest in various privacy-related topics by writing to the Special Rapporteur and/or requesting meetings, most of which were granted. These meetings have enabled the Special Rapporteur to construct lists of stakeholders in various sectors and to use these lists to invite

stakeholders to meetings around the world. Structured consultations are often held behind closed doors (at the behest of stakeholders) but can include a mix of invitees and people who write in to request to attend a publicized event.

43. Furthermore, the Special Rapporteur has created structures for further investigation and consultation by setting up five Working Parties, one each for the Thematic Action Streams identified in the first set of five priorities: Big Data and Open Data; Security and Surveillance; Health Data; Personal data processed by corporations; and "A better understanding of Privacy". These will provide the basis for thematic reports, which are expected to start being presented in 2017-2018. This methodology has permitted the Special Rapporteur to partly overcome resource constraints by tapping into a global pool of experts prepared to provide their domain expertise on an unpaid volunteer basis. The Special Rapporteur will, however, continue to seek extramural funding and welcomes all forms of assistance to carry out his mandate properly.

44. The present report is constrained by the imposed arbitrary word limit and has left out commentary on at least a dozen areas on which the mandate holder has worked. These areas will hopefully be developed further in future thematic and generic reports.

45. While broadly satisfied with the collaboration to date, the Special Rapporteur recommends that more governments engage with the mandate and, as other governments have done during the first year of activity, come forward to consult on draft privacy laws and related areas such as surveillance when these are still at an early stage. Furthermore, the Special Rapporteur strongly encourages and appreciates participation in, and facilitation of, initiatives organized by the mandate holder, such as IIOF2016 or informal country visits or various workshop conferences.